GCED$^{\text{Q\&As}}$

GIAC Certified Enterprise Defender Practice Test

Pass GIAC GCED Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/gced.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

What does the following WMIC command accomplish?

process where name=\\'malicious.exe\\' delete

A. Removes the `malicious.exe\\' process form the Start menu and Run registry key

B. Stops current process handles associated with the process named `malicious.exe\\'

C. Removes the executable `malicious.exe\\' from the file system

D. Stops the `malicious.exe\\' process from running and being restarted at the next reboot

Correct Answer: B

QUESTION 2

A company wants to allow only company-issued devices to attach to the wired and wireless networks. Additionally, devices that are not up-to-date with OS patches need to be isolated from the rest of the network until they are updated. Which technology standards or protocols would meet these requirements?

A. 802.1x and Network Access Control

B. Kerberos and Network Access Control

C. LDAP and Authentication, Authorization and Accounting (AAA)

D. 802.11i and Authentication, Authorization and Accounting (AAA)

Correct Answer: A

QUESTION 3

Which Windows tool would use the following command to view a process: process where name=\\'suspect_malware.exe\\'list statistics

A. TCPView

B. Tasklist

C. WMIC

D. Netstat

Correct Answer: C

QUESTION 4

What would a penetration tester expect to access after the following metasploit payload is delivered successfully?

Set PAYLOAD windows / shell / reverse _ tcp

A. VNC server session on the target

B. A netcat listener on the target

C. A meterpreter prompt on the target

D. A command prompt on the target

Correct Answer: D

Explanation: set PAYLOAD windows/shell/reverse_tcp should get you to a command prompt on the host system. A different payload is used to get a meterpreter session. This payload does not start a VNC server or netcat listener on the target system.

QUESTION 5

Which type of attack could be used to obtain IOS router configuration files without a valid user password?

A. ARP cache poisoning

B. CDP sniffing

C. SNMP man in the middle

D. TFTP brute force

Correct Answer: D

Explanation: TFTP is a protocol to transfer files and commonly used with routers for configuration files, IOS images, and more. It requires no authentication. To download a file you need only know (or guess) its name. CDP, SNMP and ARP are not used for accessing or transferring IOS configuration files.